UNITED STATES PATENT AND TRADEMARK OFFICE

am

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/805,299	03/12/2001	Virginia L. Robbins	42390P10446	2107

8791 7590 06/14/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
KLIMACH, PAULA W	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 06/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/805,299	**Applicant(s)** ROBBINS ET AL.	
	Examiner Paula W. Klimach	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 March 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21,24,26-28 and 30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21,24,26-28 and 30* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 03/29/05 has been entered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 7-11, and 17-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slavin (5,956,407) in view of Leppek (5,933,501) and further in view of Kousa (4,797,672).

In reference to claim 1, 7, 17, and 21, regarding the decryption generating section coupled to the key generating section and a main decryption section, the decryption generating section generating a plurality of individual decryption processes based on the main decryption section and the plurality of individual keys. The monitors disclosed by Slavin generate a plurality of individual decryption processes that are based on the main decryption section. The individual processes use the values of p2 and or q2 that were provided to the monitor to decrypt and therefore eavesdrop on the transmitted information. The receiver calculates and publishes the different decryption processes En used by the monitor, which are based on the main decryption section's public and private keys (Fig. 2 and Fig. 3).

Regarding each of the plurality of individual decryption processes being different from one another, although Slavin discloses a system that creates a decoding key as a function of the prime factors used to create the encoding key (column 6 lines 31-34), Slavin does not expressly disclose individual decryption processes that are different form one another.

Leppek disclose a system that combines a selected plurality of different encryption operators stored in an encryption operator database into a compound sequence of encryption operators (abstract). Therefore Leppek discloses a system that generates a plurality of individual decryption processes wherein each decryption process is different from one another (column 4 lines 33-67). The system uses one key in conjunction with only a one of the plurality of decryption processes (Fig. 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add a system for creating a plurality of encryption sequences as in the system of Leppek to system of creating a plurality of keys of Slavin. One of ordinary skill in the art would have been motivated to do this because it would scramble the data stream having no readily discernible encryption 'footprint' (column 2 lines 25-38).

Regarding the main encryption section, the main encryption section using the main key to encrypt content. The sender encrypts the message using Eun.

Slavin does not disclose the different parts disclosed above as belonging in the same circuit. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to create a system that receives and transmits therefore including all the parts as disclosed above in the same circuit. One of ordinary skill in the art would have been motivated to do this because it would secure the transmitted information as well as the information that is received by synchronizing the distribution of key.

Although Slavin discloses a key generation section that generates section to generate a plurality of individual keys based on a main key each based on a main key and different from one another, Slavin does not disclose only one of the plurality of individual keys is used in the decryption processes.

Kousa discloses a system that generates a plurality of keys from a master key (seed) wherein only one of the plurality of individual keys is used in conjunction with only one decryption processes (column 4 lines 30-53).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate a plurality of keys from a master key and use it with one decryption process as in Kousa in the system of Slavin. One of ordinary skill in the art would have been motivated to do this because it provides increased security from unauthorized access by others (Kousa column 6 lines 60-67).

In reference to claims 2, 8, 18, wherein each of the plurality of individual decryption processes each use a selected one of the plurality of individual keys. Fig. 2 discloses the monitor only being provided with p2, which is used to calculate the key and then decrypt that data.

In reference to claims 3, 9, wherein the plurality of individual decryption processes decrypt the content from the cypher-content by using the plurality of individual keys. Column 4 line 40 discloses providing the monitor with p2 and q2. Since two keys that depend on the main key are provided, this number could be increased to more.

In reference to claims 10 and 19, wherein the encrypting generates cipher content from the content (Fig. 5).

In reference to claims 11 and 20, wherein the plurality of individual decryption processes decrypt the content form the cipher-content by using the plurality of individual keys (Fig. 5 section describing the activity of the monitor).

Claims 4-6, 12-16, 24, 26-28, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kousa in view of Leppek and Morris et al (4,503,287).

In reference to claims 4, 12, 24, and 28, Kousa discloses a system for generating a plurality of individual keys based on a main key (seed), each of said plurality of individual keys being different from one another (column 2 lines 3-45).

Regarding each of the plurality of individual decryption processes being different from one another, although Kousa discloses encrypting information between the base and the node using the plurality of keys, Kousa does not disclose generating a plurality of individual decryption processes based on a main decryption process and.

Leppek disclose a system that combines a selected plurality of different encryption operators stored in an encryption operator database into a compound sequence of encryption operators (abstract). Therefore Leppek discloses a system that generates a plurality of individual decryption processes wherein each decryption process is different from one another (column 4 lines 33-67). The key is sent to the system of Leppek and therefore key generator is coupled to the encryption generating section (fig. 2 part 170).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add a system for creating a plurality of encryption sequences as in the system of Leppek using the plurality of keys generated by the system of Kousa. One of ordinary skill in the art would have been motivated to do this because it would scramble the data stream having no readily discernible encryption 'footprint' (column 2 lines 25-38).

Although the system of Kousa discloses a system wherein the Master key is known, Kousa does not disclose the main decryption section using the main key to decrypt cipher-content.

Morris discloses a system wherein the main key (Master key) is used to decipher the session encryptor key, which is transmitted as cipher text (column 4 lines 39-43).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to decrypt the session cipher text as in Morris in the system of Kousa. One of ordinary skill in the art would have been motivated to do this because the Master key is the same in the terminal and the host and therefore can be used to send the session key safely from one device to another using encryption.

In reference to claims 5 and 13 wherein the plurality of individual encryption processes to each use one of the plurality of individual keys.

Leppek disclose a system that combines a selected plurality of different encryption operators stored in an encryption operator database into a compound sequence of encryption operators (abstract). Therefore Leppek discloses a system that generates a plurality of individual decryption processes wherein each decryption process is different from one another (column 4 lines 33-67). The key is sent to the system of Leppek and therefore the system uses one key (fig. 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add a system for creating a plurality of encryption sequences as in the system of Leppek using the key generated by the system of Kousa. One of ordinary skill in the art would have been motivated to do this because it would scramble the data stream having no readily discernible encryption 'footprint' (column 2 lines 25-38).

In reference to claims 6, 14, and 30, wherein the plurality of individual encryption processes encrypt the content forming the cipher-content by using the plurality of individual keys.

Leppek disclose a system that combines a selected plurality of different encryption operators stored in an encryption operator database into a compound sequence of encryption operators (abstract). Therefore Leppek discloses a system that generates a plurality of individual decryption processes wherein each decryption process is different from one another (column 4 lines 33-67). The encryption processes generated by Leppek encrypt the content forming the cypher-content (column 5 lines 34-52).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add a system for creating a plurality of encryption sequences as in the system of Leppek using the key generated by the system of Kousa. One of ordinary skill in the art would have been motivated to do this because it would scramble the data stream having no readily discernible encryption 'footprint' (column 2 lines 25-38).

In reference to claims 15 and 26, wherein the decryption process generates a content from the cipher content. The system of Morris generates the session key from the encrypted session key.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to decrypt the session cipher text as in Morris in the system of Case. One of ordinary skill in the art would have been motivated to do this because the Master key is the same in the terminal and the host and therefore can be used to send the session key safely from one device to another using encryption.

In reference to claims 16 and 27, wherein the plurality of individual encryption processes encrypt the content forming the cipher-content by using the plurality of individual keys.

Leppek disclose a system that combines a selected plurality of different encryption operators stored in an encryption operator database into a compound sequence of encryption operators (abstract). Therefore Leppek discloses a system that generates a plurality of individual decryption processes wherein each decryption process is different from one another (column 4 lines 33-67). The encryption processes generated by Leppek encrypt the content forming the cypher-content (column 5 lines 34-52).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add a system for creating a plurality of encryption sequences as in the system of Leppek using the key generated by the system of Kousa. One of ordinary skill in the art would have been motivated to do this because it would scramble the data stream having no readily discernible encryption 'footprint' (column 2 lines 25-38).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Thursday, June 02, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100